



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/999,766	07/23/1997	SCOTT A. MOSKOWITZ	2377/23	4344

29693 7590 12/10/2002

WILEY, REIN & FIELDING, LLP  
ATTN: PATENT ADMINISTRATION  
1776 K. STREET N.W.  
WASHINGTON, DC 20006

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 12/10/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

08/999,766

Applicant(s)

MOSKOWITZ ET AL.

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 10 October 2002.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 25-63 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 25-63 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is in response to the request for reconsideration filed 04 October 2002.

### ***Response to Arguments***

2. Applicant's arguments filed 04 October 2002 have been fully considered but they are not persuasive.
3. In response to the 112 rejection, applicant cites parts of pages 18-24. This section supports a key that is based on a sample window size and a random seed. Applicant concludes by saying that "message data itself is part of the key in that it is placed within the carrier data." Applicant gives no explanation for why message data that is or will be placed in carrier data should be considered part of the key. Applicant cites no section of the specification supporting this conclusion. As such, the 112 rejection is maintained.
4. Applicant cites several perceived inconsistencies in the examiner's discussion of the initialization of the stega-cipher, specifically that  $f$  is not a random function, but uses random variables. The use of random variables does not make a function random. The output of the function would probably be random, but the function itself is not random. Applicant follows by saying that one simple explanation for how the stega-cipher creates a unique output even when using the same exact input is that the starting point of the encoding is random. The starting point of the encoding is an input; as such, applicant is

again requested to assert that the stega-cipher creates a unique output even when using the same exact input.

5. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., keys that can be either symmetric or asymmetric) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

6. In arguing against the rejection of claims as anticipated by Bender et al., applicant cites portions of the application (p. 7, lines 13-25), shows elements present in only Bender et al. (Bender at 172), and concludes that Bender et al. do not show a stega-cipher. None of these arguments draw a distinction between the claims and the reference. Applicant relies on material outside of the claims, specifically a definition not supported by the specification, as showing the patentability of the application. As has been stated before, limitations outside of the claims will not be read into the claims. The reason for this should be apparent from applicant's definition. Not only is it unsupported, the language of the definition would, if incorporated into the claims, be indefinite because of ambiguities caused by words such as "or" and "potential". Furthermore, applicant has changed the definition of stega-cipher as prosecution has proceeded. Currently, the definition includes the clause "generate[s] a key", a limitation absent from the definition given in the interview summary (paper 26). Given the shifting

nature of the definition, the examiner has relied on the claim language to determine the scope of the claim.

7. Applicant presents four alleged differences between Powell et al. and the claims. In support of the first ("Powell does not disclose the use of a cipher"), applicant says that choosing signature points randomly (as taught by Powell et al.) is not the same as using a cipher to determine which extrema will be used. This naked assertion is unsupported. In fact, the signature points in Powell et al. are extrema (pg. 4, lines 38-42), and randomly choosing points reads on using a cipher for selection. As such, Powell et al. does use a cipher to determine which extrema will be used.

8. Applicant's next argument ("Powell does not disclose the use of a key") ignores the random choice of signature points, which reads on a key. Applicant bases this argument on Powell et al. retrieving the embedded data with the original, unaltered image. While this is one way to decode the embedded data, it is not the only, as can be seen from Powell et al. (line 57 of page 5 – line 14 of page 6).

9. Applicant's third argument ("Powell does not embed independent data into a carrier signal") fails to differentiate between the independent data in Powell et al. (the signature) and the way in which it is represented (by adjusting, for example, luminance). An apparent extension of applicant's argument is that any change to the carrier signal would make the embedded signal dependent upon the carrier. Of course, applicant's invention embeds data in a carrier signal, and thus this argument seems to be irrelevant to not only Powell et al., but also the instant invention.

10. Applicant provides no explanation for the rationale behind the final argument ("Powell does not disclose a relationship between the message, signal and key or cipher"). Powell et al. do, in fact, disclose a relationship between the message, signal, and key or cipher. The message is embedded into the signal according to the key.

11. Applicant challenges the examiner's description of Powell et al. and Bender et al. as "encrypting" watermark data into the carrier signal. While this usage is correct because Powell et al. use cryptographic techniques (specifically a random selection scheme) to embed data and Bender et al. alter the to-be-embedded signal according to a pseudo-random signal, the concept of "encrypting" watermark data into a carrier signal as done by Powell et al. and Bender et al. will from hereon be read as meaning that watermark data is embedded into a carrier signals using techniques derived from cryptography and steganography.

12. Applicant's arguments with respect to DES allege that there is little resemblance between the claimed mask set and the key breakdown and permutations in DES. No support or reasoning for this conclusion is provided. In contrast, the examiner has pointed to specific portions of the DES key as specifically corresponding to the various limitations in applicant's claims. Applicant also mischaracterizes the application of DES to Powell et al.; the watermark is taught as being a candidate for encryption. It would then be embedded into Powell et al.'s image. Furthermore, the image embedded with the encrypted watermark could then be encrypted for further security.

13. Applicant's argument for rescinding the rejection of claims 52-57 is unpersuasive because it supports the rejection. According to applicant, Barton teaches unique

identification of underlying data. The unique identification is included with the signature (5912972, col. 4, lines 18-33). As such, the watermark that is added to Powell et al. would include a unique data, as required by the claim. Similarly, applicant's arguments with respect to Barton as it has been applied to Bender et al. are unpersuasive.

14. With respect to applicant's comments on Braudaway et al., Braudaway et al. use watermarking planes, which render obvious one-to-one watermarking maps.

15. Applicant's comments with respect to Bender et al. and Schneier are unpersuasive for the same reason that applicant's comments with respect to Powel et al. and Schneier are unpersuasive.

16. Encryption of the carrier signal embedded with a watermark anticipates claim 34.

17. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, added security would motivate one to incorporate the teachings of Schneier into Powell et al.

18. In response to applicant's arguments that Barton cannot be combined with Powell et al. and that Morris, Powell et al. ('377), Braudaway et al., Schneier, or Cox cannot be combined with Bender et al., the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the

primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

***Claim Rejections - 35 USC § 112***

19. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

20. Claims 25-63 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. There is no teaching of using the watermark to form the key.

***Claim Rejections - 35 USC § 102***

21. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

22. Claims 25, 27-29, 31-33, 35, 62, and 63 are rejected under 35 U.S.C. 102(a) as being anticipated by Bender et al. ("Techniques for data hiding").



In their introduction on page 164, Bender et al. distinguish between data hiding and encryption. They also state that hidden data should be "invisible" or "inaudible", which meets the limitations of claims 62 and 63. In the first paragraph of the next page, they say that watermarks are one type of data often inserted into files. In section 3.4, which studies spread spectrum environments, a pseudo-random key used to hide information is disclosed. The key, a carrier wave, and data are all combined. In section 1.2, Bender is mentioned as encrypting the embedded data. A reading of the section cited as support for the amendment of 17 January 2001 seems to say that this feature is not inherent to a stega-cipher, but it is not quite entirely clear.

23. Claims 25-33, 35-39, 62, and 63 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Powell et al. (EPO 0 581 317 A2). See page 4, lines 4 and 40-42.

***Claim Rejections - 35 USC § 103***

24. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

25. Claims 34, 40-43, and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Schneier.

Powell et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and

permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES' mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

26. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Powell et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a

person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Powell et al. and Schneier's system.

27. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Powell et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Powell et al. and Schneier. Operating on only the start of message delimiter would hide data but decrease the reliability of authentication.

28. Claims 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. in view of Barton.

Powell et al. teach encrypting digital watermarks into information. They do not say that the watermarks are each unique. In lines 20-33 of column 4, Barton teaches including sequence data with authentication data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

29. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Powell et al. and Barton as applied to claim 54 above.

Powell et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as verification. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

30. Claims 26, 30, and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Barton.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information includes a stream of digital samples. Barton's teaches embedding authentication information within a stream of digital data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to authenticate digital sample streams as in Barton with the key-encrypted watermarks of Bender et al.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that each sample has unique watermark information. In lines 20-33 of column 4, Barton teaches including sequence data with the authentication data. The authentication data is a reduced representation of digital data. Therefore it would have

been obvious to a person of ordinary skill in the art at the time the invention was made to uniquely identify different samples so that the samples can be placed in the correct order. Unique watermarks could also deter cryptanalysis attacks.

Pre-processing sample windows is inherent, as is determining which and how many windows will contain watermark information.

31. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not say that the information is then modified. Encryption modifies data. Official notice is taken that encrypting information in order to protect the data from unauthorized viewing is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect the watermarked data of Bender et al. by encrypting it.

32. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Morris.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that one bit is read out of every sample for the watermark. In lines 50-52 of the third column, Morris says that the human ear cannot detect the difference between a sound value of 64000 and 64001. This would be a one-bit change of the least significant bit. As taught by Morris, these small changes can be used to carry identification codes. Therefore it would have been obvious to a person of ordinary skill

in the art at the time the invention was made to discretely carry the watermark information of Bender et al. in the least significant bits as taught by Morris.

33. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Powell et al. (5930377).

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that samples are mapped to extract bits of information. As is explained in their abstract and diagrams, Powell et al. teach a method of embedding a digital watermark that requires use of a map of an image to determine the places to embed the watermark. This method is advantageous because, as explained in lines 42-43 of column 1, it is resistant to image modification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the mapping techniques of Powell to the encryption system of Bender et al. so as to make the data's watermark resistant to data modification.

34. Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Braudaway et al.

Bender et al. teaches encrypting digital watermarks into information with a key. He does not set out that the watermark is used in any specific manner.

By watermarking the data, Braudaway et al.'s method creates a first derivative encoded signal. It is inherent that attempts to decode the watermark without the proper key would further obfuscate the information. It was once theorized that encrypting information with two keys in order to strengthen security could in fact be mimicked by using one key that would possibly be easier to break. Although this theory has since

been proven incorrect, the immediate solution was to strengthen security by encrypting with a first key and then decrypting with a non-corresponding second key. Providing information is inherent.

In the abstract, Braudaway et al. say that certain pixels brightness are altered as a result of the watermark. This change in brightness anticipates claim 38's spectral values. Also in the abstract, Braudaway et al. talk about using only certain non-transparent values of the watermark. These non-transparent values form a map to meet claim 39.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate any of the teachings of Braudaway into Bender et al.

35. Claims 40-43 and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. in view of Schneier.

Bender et al. teaches encrypting digital watermarks into information with a key. They do not say that mask sets are used.

Chapter 10 of Schneier deals with the Digital Encryption Standard. DES uses an effectively 56-bit key. As described on pages 224-226, this key is broken down and permuted in the encryption of a block of data. This key breakdown and the subsequent permutations correspond to applicant's mask set. DES uses starting vectors and padding at the end of messages. These correspond to the start of message delimiter and number of bytes to follow the message of applicant's invention. DES uses 64-bit block encryption and divides the blocks into two 32-bit sections for encryption. This anticipates applicant's claims 42 and 47. Claims 43 and 48 are anticipated by DES'

mixing of the two 32-bit blocks and the integration of the key. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the key-encrypted watermark data of Schneier with DES because DES is an encryption standard.

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use mask sets to protect data.

36. Claims 44, 45, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier in view of Cox et al. ("Secure Spread Spectrum Watermarking for Multimedia").

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that the data is spectrally spread before insertion of the digital watermarked. In their abstract, Cox et al. talk about the advantages, which include versatility, difficulty of watermark removal, and robustness, of their system of spectrally spreading data, inserting the watermark, and then putting the watermarked data through an inverse spectral spread. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to reap the benefits of Cox et al.'s method in Bender et al. and Schneier's system.

37. Claims 50-51 and 58-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Schneier as applied to claims 41, 48, and 29 above, and further in view of Barton.

Bender et al. and Schneier teach encrypting digital watermarks into information with a key. They do not say that a digital signature or hash of the start of message



delimiter is validated. In his second figure, Barton shows a digital signature being used as an authentication tool. Digital signatures are made so that they are unique to the article that they authenticate. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use a digital signature, as taught by Barton, to verify the message sent by Bender et al. and Schneier.

38. Claims 55-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bender et al. and Barton as applied to claim 54 above.

Bender et al. teach encrypting digital watermarks into information with a key. They do not say that the data that is watermarked is hashed and attached to itself. Official notice is taken that hashing data and then attaching the hash to the data is old and well-known. The hash acts as a verifier. Digital signatures with message appendix are a common term implementation of this. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to attach a hash of the information to the information. This hash would be used to verify the integrity of the information.

### ***Conclusion***

39. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

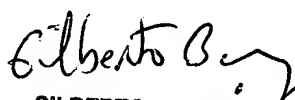
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.



DJM

December 6, 2002

Douglas J. Meislahn  
Examiner  
Art Unit 2132

  
**GILBERTO BARRÓN**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**